INFORMATION SECURITY POLICY

1. OBJECTIVE AND SCOPE

The purpose of this policy is to establish the general framework for the protection of information managed, stored, and processed by S4A, a design organization in the aeronautical field (DOA, Design Organization Approval), in such a way that the confidentiality, integrity, and availability of information are preserved, and the cyber resilience of the systems supporting aeronautical design processes is ensured, in compliance with Commission Delegated Regulation (EU) 2022/1645

2. DEFINITIONS AND ACRONYMS

TERM	DESCRIPTION
ISMM	Information Security Management Manual
ISMS	Information Security Management System

3. DECLARATION

The Senior Management of SOLUTIONS FOR AVIATION S.L., aware of the importance of aviation safety as well as information security as a fundamental strategic asset for the continuity, competitiveness, and reputation of our organization, expresses its full commitment to the design, implementation, maintenance, and continuous improvement of the Information Security Management System (ISMS), in accordance with the requirements of COMMISSION DELEGATED REGULATION (EU) 2022/1645 in its PART-IS.D.OR.

We commit to:

1. **Always working in accordance with the Annex** "Information Security. Organization Requirements [PART-IS.D.OR]" of COMMISSION DELEGATED REGULATION (EU) 2022/1645, as well as with the Information Management System Manual (IMSM).
2. **Protecting the confidentiality, integrity, and availability** of the organization's information, as well as that of our clients, partners, employees, and other stakeholders.
3. **Applying and maintaining an effective information security management system** capable of properly managing risks that may impact aviation safety.
4. **Complying with applicable legal, regulatory, and contractual requirements** regarding information security.
5. **Allocating the necessary resources** (human, technical, and financial) to ensure the effectiveness of the ISMS.
6. **Ensuring that all necessary personnel are committed** to the ongoing compliance with these requirements.
7. **Promoting continuous awareness and training** of personnel regarding information security.
8. **Establishing measurable objectives** and reviewing them periodically to ensure the continuous improvement of the system.

9. **Supporting the roles responsible for information security**, ensuring they have the appropriate authority and means for its management.
10. **Leading by example**, integrating information security at all levels of decision-making.

This letter represents our firm support and leadership in the commitment to safeguard information assets and ensure a trustworthy environment for our operations and business relationships.

This policy was signed by the Head of Design Organization in Madrid, on July 15, 2025